Contextual Healing: Privacy through Interpretation Management

Rula Sayaf
Dept. of Computer Sciences
KULeuven
Email: rula.sayaf@cs.kuleuven.be

Sören Preibusch
Google Inc.
California
Email: preibusch@google.com

Dave Clarke
Information Technology
Uppsala University
Email: dave.clarke@it.uu.se

***Abstract*—Contextual privacy is an essential concept in social software communication. Managing privacy in social software strongly depends on the context to avoid misappropriation of data. The sheer amount of data and large audiences make context control complex. Current contextual privacy management approaches can be either too complex to use, or too simple to offer fine-grained control. In many cases, it is challenging to strike a balance between effective control and ease-of-use. Moreover, current approaches are insufficient to mitigate data misappropriation attacks. In this article, we analyse contextual privacy in relation to context and communication. We examine a relevant contextual privacy management framework based on the maintenance of the interpretation of data. We propose an architecture based on the utilisation of artificial intelligence mechanisms. We conceptually analyse the usability aspects of the proposed architecture, and present how the framework enhances communication and privacy.**

I. Introduction

The surge of social software is associated with increasing complexity of managing privacy. People disclose their data to socialise and communicate with others. By a data disclosure, a user expresses a particular communicative message. A message can be communicated to large audiences. Through such communication, the user builds a desired online identity. When a user discloses data, the user controls who can view it to mitigate privacy concerns. However, with the sheer amount of data disclosure, and the mix of audiences in social software, data misappropriation concerns emerge. Data misappropriation can be illustrated in the following scenario:

Scenario 1 Some Facebook users suffered from privacy violations by the misappropriation of their profile photos—that are by default public—in the incident of 'prostitutes of Antwerp' [1]. Profile photos of girls were put in a page entitled 'prostitutes of city of Antwerp'. The possible interpretation in the new context negatively affected the identity of the girls and counted as a privacy violation and was reported to the authorities as well as Facebook [1]

The scenario demonstrates how misappropriation can occur in private and public spaces. Private spaces are those in which accessibility is limited to a specific set of audience. The audience are trusted not to disseminate the data. However, a member can act adversarially and misappropriate the data if the data owner is not able to limit dissemination in all possible inappropriate contexts. Misappropriation can occur when a data item is shared publicly because the user has no means to fully control data dissemination. Problems of dissemination control emerge from insufficient degree of control over context [2].

Misappropriation of data is a particular class of attacks that current privacy management approaches do not fully address. Misappropriation of data is the result of any act that changes the context of data to an inappropriate context. Traditionally, attacker models focus on actions that change the information and knowledge state of the attacker. However, a misappropriation attacker model focuses on achieving an inappropriate state of the data. Countering such an attack is not possible currently because privacy management approaches aim at only prohibiting or allowing particular actions, but they do not focus on assessing the appropriateness of data after an action. To address such an attack, we need to include means to assess the appropriateness of data without burdening users. We propose utilising artificial intelligence to assist users [3] through a previously proposed framework for contextual privacy for social software (CPS^2) [4]. The framework offers privacy management through managing the interpretation of data. This article contributes the following:

1) An analysis of context control issues, and the attacker model of misappropriation (Section II)
2) An analysis of contextual privacy concepts (Section III)
3) An architecture design for CPS^2, a discussion of a possible implementation using deep learning, and a conceptual analysis of the framework usability aspects (Section IV).
4) A discussion of how the proposed framework can be applied to enhance privacy and communication (Section V).

II. Problem Statement

This section discusses the problem of managing privacy by controlling context, and presents the attacker model.

A. Issues of Context Control

Managing privacy and mitigating misappropriation of data requires a high degree of context control. From a 'privacy as control' point of view [5], privacy is achievable through controlling the data and the context wherein data is put. However, most privacy management approaches offer limited control over the disclosure context [2]. Mitigating misappropriation

requires prohibiting data dissemination in inappropriate contexts. Such mitigation requires specifying the set of appropriate and inappropriate contexts. This specification is infeasible due to the theoretically infinite number of contexts [4].

Simplified means of contextual privacy management are insufficient to mitigate data misappropriation [6]. To avoid the complexity of context control, most approaches adopt simple means of context control. The simplification is achieved by capturing context by a few parameters [6], such as roles of users [7], location or time [8]. This results in offering limited control over the disclosure context, and a lower degree of control over dissemination context [2]. Consequently, users cannot control every change of the contexts their data is in to avoid inappropriate changes. When context changes, the sensitivity of data may increase, and thus, the data owner may incur privacy violations. Controlling context change is even more challenging when context is unclear. Social software contexts can possibly be ambiguous due to the mix of audiences and data [9]. In such situations, it may not be possible to assess the sensitivity and the appropriateness of data. Incorrect assessment of appropriateness can even result in an unintentional misappropriation attack. Current privacy management approaches are not sufficient to counter this attack, whether it is intentional or not, due to the complexity of controlling context.

B. Attacker Model

A misappropriation attack is achieved by any act that affects the user's communicative message, according to the following model:

- A (trusted) system: is the social software system that facilities social communication functions. The system enforces users' privacy policies and allows actions that are not prohibited otherwise by the data owner.
- A data owner: is the user who discloses a data item to communicate a message and is targeted by the attacker
- An attacker: is the user who can access the data item, and by performing a particular action, the context changes and becomes inappropriate for the data of the attacked user. The change can be achieved by putting the data in a new context, or by causing the current context to evolve through an action of adding or removing data from the context. An example is when Alice posts her *breast-feeding* photo in a *breast-feeding* context, and Bob (the attacker) changes the context to an *adult* context by adding a comment that changes the conversation topic.

In theory, misappropriation attacks can be prevented by monitoring actions on data. In practice, monitoring and detecting attacks requires complete information about all users' actions. However, data owners cannot monitor and know all actions of other users. Given the limited context control and the incomplete information of data owners, it is required to integrate artificial intelligence approaches to detect such attacks. Towards proposing such an approach, an analysis of the role of context in privacy management and communication is discussed next .

III. Contextual Privacy

This section illustrates contextual privacy as a means to manage the communication context to protect privacy.

A. Context

Context is "any information that can be used to characterise the situation" [10]. An online context is any information that can be used to characterise an online situation. The context implies the topic of communication and possibly some characteristics of the interlocutors. A context can be approximated by the set of available informational parameters in the situation. We refer to those parameters as *the context-approximation parameters* (CAP). The inaccessibility of these parameters hinders the correct approximation of context, and the context is *ambiguous*. A situation in social software can be characterised by a post and a context wherein the post is put (Fig. 1(a)). The communication context includes the data surrounding the post, the data owner and an audience.

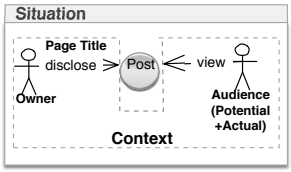
By controlling context, it is possible to affect the approximation of context and the interpretation of data. Adding or removing data to context can affect the CAP, and as result the context changes. Whenever the observer—a member of the audience—is unaware of this change, there can be discrepancy between the *perceived* and the *actual* context resulting in ambiguity (Fig. 1(b)). Ambiguity disrupts the interpretation of the communicated message. By controlling the CAP, the correct inference of the context can be facilitated.

Context provides the appropriate interpretation in a situation [11]. The interpretation captures the meaning or the message, as well as the sensitivity of a data item [12]. A data item can have a limited set of possible interpretations. Based on the context, the relevant interpretation can be disambiguated [13]. When the post is put in a certain context (we say 'contextualised' [14]), the interpretation implicitly reflects that the post is in that context (Fig. 1(b)). Decontextualisation is the process of taking a post out of the current context, to where the interpretation is unavailable [14]. We identify the third process of moving posts between two contexts as *recontextualisation*. Such a process decontextualises a post and contextualises it in another.

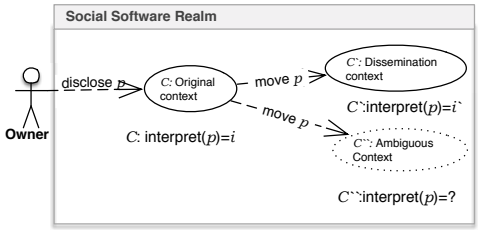
B. Communication in Social Software

In most communication situations, people aim at conveying a particular message. The successful delivery of the communicative message to the audience can affect privacy. To understand such an effect, we focus on two extreme ends of the communication spectrum, namely, cooperative and adversarial communication. These types emphasise the varying roles of context and privacy, as we discuss in the following.

1) Cooperative Communication: In cooperative communication, the interlocutors cooperate to understand the meaning of the communicated message. According to Grice, facilitating the inference of a message requires the interlocutors to cooperate and put an effort to clarify the communication context [15]. Grice stated that providing true, relevant, and sufficient amount of information while avoiding ambiguity are



(a) A simplistic representation of a communication situation.



(b) The post p is disclosed in C, where it has the interpretation i. When p is in C', the *dissemination* context, the interpretation is i'. When p is in the ambiguous context C'', an observer may not be able to interpret p.

Figure 1: Context in social software.

key to unambiguous context. In this communication, privacy concerns are relatively low because context is clear and the interlocutors trust each other clarify a misinterpretation.

2) Adversarial Communication: Adversarial communication is characterised by the manipulation of the communicated message. An interlocutor—the adversary—acts maliciously and misleads others into misinterpreting the message to disrupt the communication or force others to reveal certain information [16]. Alternatively, when context is ambiguous, communication can also become adversarial [17]. In such communication, users can protect privacy by providing less information [18], with detrimental consequences on the clarity of context and the inference of the communicative message. Such a strategy may result in a misinterpretation of data, and hence an unintentional adversarial communication, or an unintintional attack (Scenario 7). In this communication, privacy concerns are high, the degree of trust is low, and data interpretation is manipulated.

C. Identity and Privacy

The act of communication is related to expressing a desired identity [19]. Privacy as control is demonstrated as informational self-determination and facilitates identity management [20]. The communicated message of a user contributes, in turn, to the identity a user is expressing [21]. The misappropriation attacker aims at affecting the identity of the attacked user's. To mitigate the attack, contextual privacy should guarantee that the communicated message can be correctly inferred to avoid misinterpretation leading to identity damage.

IV. Managing Contextual Privacy

The observed interdependence of privacy and communication in the previous section validates the previous conceptualisation of contextual privacy by Sayaf et al. [4]. This interdependence suggests that by maintaining the interpretation of a data item, privacy can be maintained. By using the interpretation to manage contextual privacy, the complexity of controlling context can also be overcome. Given the limited possibilities of data interpretation, it is easier for users to specify the appropriate interpretations, than to specify the appropriate contexts. If it is possible to observe the interpretation of a post by means of automatic context and interpretation inference tools, it would be possible for users to have control over context without having to continuously monitor context and possible attackers.

A. CPS^2: Contextual Privacy Framework for Social Software

The previously proposed framework CPS^2 is a conceptual framework to manage contextual privacy and counter the misappropriation attack. It assumes that the interpretation in a specific context is *appropriate* if the owner allows the disclosure in this context. CPS^2 states that an owner can specify the appropriate interpretation of her post, and based on this interpretation, dissemination and context changes can be controlled automatically, and attacks can be detected. By specifying the appropriate interpretation, the framework facilitates the inference of the intended interpretation by the audience.

B. An Architecture Design for Contextual Privacy Management

In this section, we propose an architecture design for CPS^2. The framework lifts the burden of reasoning about context to the level of the social platform, and proposes three layers to manage contextual privacy. We present the interaction between these layers (Fig. 2), and investigate techniques of machine deep learning to implement inference layers.

1) Context Inference Layer: processes the data of a situation to approximate the current context within the social software realm.

2) Interpretation Inference Layer: infers the interpretation of data, based on the inferred context. Inferring the interpretation is similar to how a search engine matches a search query to a document: the document is the context and the query is the post. The query has a specific interpretation in a document, based on the popularity of this interpretation, the engine judges the relevance of the document. Similarly, the interpretation of a post can be inferred in an online context.

3) Contextual Privacy Management Layer (CPML): facilitates contextual privacy management by maintaining the appropriateness of interpretation. This layer can follow two 'privacy as control' approaches, access control or accountability and auditing approaches [4]. In access control, CPML allows users to specify the appropriate interpretation of their posts. CPML verifies any action or change of context to

maintain the appropriateness of the interpretation. Alternatively, without specifying the appropriate interpretation, CPML notifies the owner when the interpretation changes, following an accountability and auditing approach. The owner judges the appropriateness of the new interpretation, and accordingly the change of context is allowed or prohibited.

The inference layers need to be embedded in the software platform. These layers can be implemented by machine learning models, especially deep machine learning generative models. Deep learning focuses on computational models for complex information representation [22]. Generative models are useful for unsupervised learning with a high number of parameters [23]. These models are useful in social software situations because the parameters are many and vary across users; and because it may not be possible to have context and interpretation labels during the training phase. Generative models can learn a joint probability distribution over observable data and labels. This means that it is possible to estimate the conditional probability $P(O|L)$ and $P(L|O)$, where L is a label and O is a set of observable data variable. In CPS^2, the observable data is the CAP, and labels are information about context names and interpretations.

One example of generative models that could be applied for inferences is the Multimodal Learning with Deep Boltzman Machine proposed by Srivastava and Salakhutdinov [24]. The model learns a multimodal data representation to perform classification and information retrieval tasks. The model classifies images and tags them; and it can also retrieve images corresponding to a set of tags. This model can be applied for context and interpretation inference, and context retrieval. A post can be classified given CAP to infer the interpretation. It is also possible to retrieve a context, or a set of CAP given an interpretation. For instance, given an interpretation—and possibly a post—the appropriate contexts can be retrieved and displayed to the user. On top of such a model, CPML can be implemented as an access control or accountability approach.

C. Conceptual Analysis of Usability

In this section, we present a comparative assessment of the usability of CPS^2 with the conceptual framework 'Privacy as Contextual Integrity' (CI) proposed by Nissenbaum [25].

Usability is an important aspect in achieving the objectives of privacy management approaches [26]. If an approach is not easy to use, average users would fail to manage their privacy. Assessing the usability of an approach is essential at the design phase. We conceptually analyse the usability of CPS^2 and CI using the'Security Usability Model' proposed by Braz et al. [26] using metrics for usability standards.

In principle, the usability of CPS^2 is higher than the usability of CI. CI addresses the issue of limiting recontextualisation of data by controlling four parameters: contexts, actors, attributes, and transmission principles. CI requires the specification of the norms including: terms of information flow; the prevailing contexts and possible sub- and super-contexts; subjects, senders, recipients; and transmission principles. CI requires specifying parameters that may be challenging to specify in advance, e.g., users may not be aware of the terms of information flow in the system, or they may not be able to predict how the terms may change over time. CPS^2 limits the number of parameters users need to specify. Thus, CPS^2 satisfies most of the metrics to a higher degree than CI (Table I).

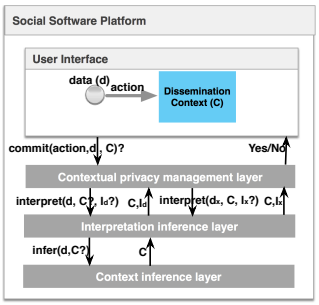


Figure 2: Interaction between layers. Upon adding a post d, CPML checks whether the action can be committed by consulting the interpretation inference layer. To infer the interpretation, the context inference layer is consulted to check if the current context changes by simulating the action. Based on the inferred context, the interpretation layer infers the new interpretation I_d. If I_d is appropriate and the context changes, CPML checks the appropriateness of the interpretations of other posts d_x before allowing the action.

D. Implications for User Interface Design and Engineering

In this work, we foresee three main design aims that enhance the user interaction experience of social software, contribute to the usability, and offer better privacy management.

- Context change alerts: Users can be alerted when CAP change. Users will be given the opportunity to prevent unwanted changes.
- Awareness tools: More generally, users will be made more aware of how their communication evolves. The communication owner will be notified of context change and be given the opportunity to act properly.
- Feedback loops: Users can have the opportunity to provide feedback to the system (e.g., rate alerts or confirm blocked audience), thereby generating labels that become part of the training data and gradually improve the system recommendations. Over time, social software will refine how the intended interpretation is concisely presented to users.

V. Applying CPS^2

In this section, we present how CPS^2 can be applied in to enhance privacy management while requiring minimal involvement of users during the following interaction phases with the software.

Usability Metric	Description	CPS^2	CI
UM1- Minimal Action	the amount of action required to achieve the task	low	high
UM2- Minimal Memory Load	the amount of information the user should have in mind to complete the task	low	high
UM3-Operability	amount of effort required to operate an application	low	high
UM4-Privacy	whether users' personal information is protected	Yes	Yes
UM5-Security	whether of the application protects information in the system against security threats		depends on the hosting system

Table I: Usability metrics. Given that this is an estimate of the performance of the designed system, we only use two degrees 'high' and 'low' to indicate the estimated degree. We omit the time metric due to lack of information about performance aspects.

1) Disclosure of a Post: The owner provides values for the various CAP, such as post attributes and the audience. The context inference layer infers the context. The interpretation layer infers a set of relevant interpretations. CPML prompts the owner with the set of possible interpretations to specify the appropriate interpretation—in case it follows an access control approach. In case it follows an accountability and auditing approach, CPML saves the inferred interpretations from the original context, or can also allow the user to specify the appropriate interpretation for accuracy.

2) Context Evolution: CPML checks changes in context and allows only those that continue to preserve the appropriateness of data interpretation. The change is simulated so that the context inference layer and interpretation layer infer the context and the interpretation after the change. Based on the appropriateness of the interpretations of all posts in the new context, CPML either allows the change, or prohibits it, in case it follows an access control approach. If the change will misappropriate the interpretation of any post and if CPML follows an accountability and auditing approach, it notifies the relevant owners to judge the appropriateness in the new context.

3) Recontextualisation: When a post is added to a situation, CPML interacts with the interpretation layer to infer the post interpretation in the new context. If the new interpretation has not been specified as appropriate by the owner of the post, the recontextualisation is prohibited. If an accountability approach is followed, the owner can judge the appropriateness.

Upon any misappropriation attack, the framework would be able to detect the misappropriation and prohibit it, or consult the attacked user.

A. Enhancing Communication

In the following we present how CPS^2 is needed to enhance privacy management in adversarial communication.

In scenario 1, the manipulated interpretation of the photo through the recontextualisation makes the communication adversarial. This type of adversarial communication can be mitigated by CPS^2 without having to adopt other strategies such as social stenography, which is demonstrated in this scenario reported by Boyd [27]:

Scenario 7 Carmen was sad because she broke up with her boyfriend. She wanted to express that to her friends but not to her mother so that she would not worry. Carmen posted lyrics from "Always Look on the Bright Side of Life" from the film "Life of Brian", where the main character is about to be killed. She knew that some of her friends would infer her exact communicated message, while her mother would infer a literal meaning of the post.

This scenario reflects how users adopt particular strategies when they are unable to control context or want to avoid investing time and effort in restricting the audience [28]. Carmen keeps the context ambiguous and chooses to disclose a post that has two interpretations so that the correct interpretation is not inferred by all the members of the audience. By doing so, she misleads those in the audience who believe she is truly happy when they are unaware of the actual context. The interpretation can be disambiguated based on the audience's knowledge with the film and the online context. This way, the post can be correctly perceived by the friends but not the mother.

The approach of Carmen is referred to as social steganography [27]. It is based on manipulating the interpretation to only convey it correctly to the appropriate audience. It is convenient for users who are faced with the complexity of privacy management approaches. It is also similar to the concept of CPS^2, yet, insufficient for contextual privacy management: any of Carmen's friends could comment in a way that reveals an interpretation that Carmen does not want to make explicit. Another problem with this approach is that it obstructs communication. The deliberate interpretation ambiguity may lead to ineffective communication It also involves the risk of inappropriate behaviour by the audience who are unable to perceive the intended interpretation. However, CPS^2 is required to avoid such consequences of social steganography, and to manage privacy more effectively.

VI. Related Work

Various works realise the importance of context in privacy management. However, most approaches lack the dynamic adaptivity to changes in context [6] by simplifying the representation of context. In the access control model proposed by Fong [29], relationships represent contexts. The context is approximated by relationships between the audi-

ence and the owner, regardless of the type and semantics of the posts they are communicating about. The contextual privacy approaches based on Nissenbaum's work [25] also simplify the representation of context to avoid the prohibitive complexity of specifying details in advance [7]. Simplifying context representation has many shortcomings. In the case of representing context by means of roles, the process is ineffective and time consuming. Users are not willing to invest time in such a process [30]. However, artificial intelligence can be used to address the challenge of assigning roles to users by utilising clustering algorithms [31]. Yet, empirical studies with Facebook users show that grouping friends in a set of classes or roles is not relevant to privacy management [32]. Thus, approaches like ours are needed to simplify contextual privacy management, and achieve a higher degree of privacy and effective communication.

VII. Conclusion

Context is an essential ingredient for communication and privacy management. This article emphasises the role of context in interpreting posts and privacy management. By managing contextual privacy through managing the interpretation of posts, users could manage their privacy without being faced with the complexity of controlling context. The proposed architecture design using intelligent mechanisms is promising for addressing the complexity of controlling context, and enhancing communication. It is promising for offering social software experience while having privacy preserved in private and public spaces with a relatively high degree of usability, as well as offering other functionalities related to feedback and awareness.

References

[1] R. De Wolf, "Over 'spotted', 'hoeren' en 'failed'-pagina's," Electronic article: http://www.knack.be/nieuws/belgie/dader-antwerpse-hoeren-foto-geklist/article-4000230766578.htm, Last checked Feb. 2013, 2013. [Online]. Available: http://www.knack.be/nieuws/belgie/dader-antwerpse-hoeren-foto-geklist/article-4000230766578.htm

[2] R. Sayaf, D. Clarke, and J. B. Rule, "The other side of privacy: Surveillance in data control," in *Proceedings of the 2015 British HCI Conference*, ser. British HCI '15. New York, NY, USA: ACM, 2015, pp. 184–192.

[3] S. Gürses and C. Diaz, "Two tales of privacy in online social networks," *IEEE Security & Privacy*, vol. 11, no. 3, pp. 29–37, 2013.

[4] R. Sayaf, D. Clarke, and R. Harper, "CPS^2: a contextual privacy framework for social software," in *SECURECOMM 2014*. Springer, 2014.

[5] S. Gürses, "Multilateral privacy requirements analysis in online social network services," Ph.D. dissertation, KU Leuven, 2010.

[6] R. Sayaf and D. Clarke, "Access control models for online social networks," *Social Network Engineering for Secure Web Data and Services*, pp. 32–65, 2012.

[7] A. Barth, A. Datta, J. C. Mitchell, and H. Nissenbaum, "Privacy and contextual integrity: Framework and applications," in *IEEE S& P'6*. IEEE Computer Society, 2006, pp. 184–198.

[8] N. Ajam, N. Cuppens-Boulahia, and F. Cuppens, "Contextual privacy management in extended role based access control model," in *Proceedings of the 4th workshop, and 2d conference on Data Privacy Management and Autonomous Spontaneous Security*. Springer, 2010, pp. 121–135.

[9] J. Meyrowitz, *No sense of place: The impact of electronic media on social behavior*. Oxford University Press New York, 1985.

[10] G. D. Abowd, A. K. Dey, P. J. Brown, N. Davies, M. Smith, and P. Steggles, "Towards a better understanding of context and context-awareness," in *Proceedings of the 1st international symposium on Handheld and Ubiquitous Computing*. Springer-Verlag, 1999, pp. 304–307.

[11] P. Brézillon, "Context in problem solving: a survey," in *The Knowledge Engineering Review*, vol. 14. Cambridge University Press, 1999, pp. 1–34.

[12] A. Analyti, M. Theodorakis, N. Spyratos, and P. Constantopoulos, "Contextualization as an independent abstraction mechanism for conceptual modeling," in *Information Systems*, vol. 32. Elsevier, 2007, pp. 24–60.

[13] V. Akman, "Rethinking context as a social construct," *Journal of Pragmatics*, vol. 32, no. 6, pp. 743–759, 2000.

[14] J. McCarthy, "Formalizing context (expanded notes)," in *Computing Natural Language*, A. Aliseda, R. J. van Glabbeek, and D. Westerstahl, Eds. CSLI Publications, 1993, pp. 13–50.

[15] H. P. Grice, "Logic and conversation," in *The Logic of Grammar*, D. Davidson and G. Harman, Eds. Harvard Univ., 1975, pp. 64–75.

[16] M. Dynel, "There is method in the humorous speaker's madness: Humour and grice's model," *Lodz Papers in Pragmatics*, vol. 4, no. 1, pp. 159–185, 2008.

[17] B. Skyrms, "Pragmatics, logic and information processing," in *Language, games, and evolution*. Springer, 2011, pp. 177–187.

[18] R. Verbrugge and L. Mol, "Learning to apply theory of mind," *Journal of Logic, Language and Information*, vol. 17, no. 4, pp. 489–511, 2008.

[19] E. Goffman, "The presentation of self in everyday life," *Garden City, NY Double Day*, 1959.

[20] L. Palen and P. Dourish, "Unpacking "privacy" for a networked world," in *Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM, 2003, pp. 129–136.

[21] E. Goffman, "The presentation of self in everyday life." *Garden City, NY*, 1959.

[22] I. Arel, D. C. Rose, and T. P. Karnowski, "Deep machine learning-a new frontier in artificial intelligence research," *Computational Intelligence Magazine, IEEE*, vol. 5, no. 4, pp. 13–18, 2010.

[23] G. Hinton, S. Osindero, and Y.-W. Teh, "A fast learning algorithm for deep belief nets," *Neural computation*, vol. 18, no. 7, pp. 1527–1554, 2006.

[24] N. Srivastava and R. Salakhutdinov, "Multimodal learning with deep boltzmann machines," in *Advances in neural information processing systems*, 2012, pp. 2222–2230.

[25] H. Nissenbaum, *Privacy in context: Technology, policy, and the integrity of social life*. Stanford Law & Politics, 2010.

[26] C. Braz, A. Seffah, and D. M'Raihi, "Designing a trade-off between usability and security: a metrics based-model," in *HCI–INTERACT 2007*. Springer, 2007, pp. 114–126.

[27] D. Boyd and A. Marwick, "Social steganography: Privacy in networked publics," *International Communication Association, Boston, MA*, 2011.

[28] A. Lampinen, V. Lehtinen, A. Lehmuskallio, and S. Tamminen, "We're in it together: interpersonal management of disclosure in social network services," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2011, pp. 3217–3226.

[29] P. W. L. Fong, "Relationship-based access control: protection model and policy language," in *Proceedings of the first ACM conference on Data and application security and privacy*, ser. CODASPY 11. New York, NY, USA: ACM, 2011, pp. 191–202.

[30] H. R. Lipford, A. Besmer, and J. Watson, "Understanding privacy settings in facebook with an audience view," in *Proceedings of the 1st Conference on Usability, Psychology, and Security*. Berkeley, CA, USA: USENIX Association, 2008, pp. 2:1–2:8.

[31] B. Gao, B. Berendt, D. Clarke, R. De Wolf, T. Peetz, J. Pierson, and R. Sayaf, "Interactive grouping of friends in osn: Towards online context management," *International Workshop on Privacy in Social Data (PinSoDa)*, 2012.

[32] P. G. Kelley, R. Brewer, Y. Mayer, L. F. Cranor, and N. Sadeh, "An investigation into facebook friend grouping," in *HCI–INTERACT 2011*. Springer, 2011, pp. 216–233.